George F. Ogilvie III (NSBN #3552)
Amanda C. Yen (NSBN #9726)
McDONALD CARANO LLP
2300 W. Sahara Ave, Suite 1200
Las Vegas, NV 89102
Telephone: 702.873.4100
Fax: 702.873.9966
gogilvie@mcdonaldcarano.com
ayen@mcdonaldcarano.com

Steven L. Procaccini (*Pro Hac Vice*)
Chris Ellis Jr. (*Pro Hac Vice*)
NISSENBAUM LAW GROUP, LLC
2400 Morris Avenue, Suite 301
Union, NJ 07083
Telephone: 908-686-8000
Fax: 908-686-8550
sp@gdnlaw.com
ce@gdnlaw.com

Attorneys for plaintiff Todd VanDeHey

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

TODD VANDEHEY, an individual, Plaintiff, v. REAL SOCIAL DYNAMICS, INC., a Nevada corporation; NICHOLAS KHO, an individual; OWEN COOK, an individual, Defendants.	CASE NO.: 2:17-cv-02230-JAD-NJK

DECLARATION OF ONDREJ KREHEL, CISSP, CEH, CEI IN SUPPORT OF PLAINTIFF'S EMERGENCY MOTION FOR A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

I, ONDREJ KREHEL, declare as follows:

1. I am the founder and chief executive of LIFARS, an international cyber security and digital forensics firm.

McDONALD CARANO
2300 WEST SAHARA AVENUE, SUITE 1200 • LAS VEGAS, NEVADA 89102
PHONE 702.873.4100 • FAX 702.873.9966

2. This declaration is made of my own personal knowledge except where stated on information and belief, and as to those matters, I believe them to be true. If called as a witness, I would competently testify thereto.

3. Prior to founding LIFARS, I was the Chief Information Security Officer of Identity Theft 911, the nation's premier identity theft recovery and data breach management service. I also previously conducted forensic investigations and managed the cyber security departments at Stroz Friedberg and the Loews Corporation.

4. I have two decades of experience in computer security and digital forensics and have launched investigations into a broad range of information technology security matters—from hacker attacks to data breaches and intellectual property theft.

Plaintiff Engaged LIFARS to Investigate Suspicious Activity in His Personal Gmail Account.

5. On or about September 11, 2017, plaintiff Todd VanDeHey ("Plaintiff") engaged LIFARS to conduct a forensic examination of his personal Gmail account "tvandehey@gmail.com" (the "Personal Email") which he believed had been accessed by third-parties without authorization.

6. Gmail is an email service provided by Google Inc.

7. LIFARS' forensic examination of the Personal Email uncovered that between on or about September 10, 2017 and on or about September 11, 2017, the following occurred in the Personal Email:

a. Suspicious events occurred in the Personal Email that were not performed by Plaintiff;

b. A full backup of the Personal Email was performed by someone other than Plaintiff;

c. Recovery information for the Personal Account was changed to an email address and phone number not controlled by Plaintiff

d. Information provided by Verizon Wireless confirmed that the recovery phone number not controlled by Plaintiff is registered to defendant Nicholas Kho ("Kho");

e. Emails were discovered in the Personal Email that had been sent to an email address that was not under the control of Plaintiff; and

f. Information provided by Google, Inc. confirmed that the IPv6 login to the Personal Email was conducted from a phone registered to Defendant Kho.

8. Details relating to LIFARS' findings are outlined below. A true and accurate copy of a log of the found artifacts for the Personal Email is attached hereto as **Exhibit A**.

Unknown Third-Parties Accessed The Personal Email.

9. On or about September 10, 2017 at 11:51 PM (all times herein are EDT), unauthorized users began a process to access and obtain information from the Personal Email without authorization. *See* Exhibit A.

10. Specifically, between on or about September 10, 2017 and September 11, 2017, those unauthorized users forwarded at least seven (7) emails from the Personal Email to the Personal Email.

11. Those unauthorized users then proceeded to delete those seven (7) emails from the "Trash" folder of the Personal Email.

12. Each of the seven (7) emails contained single attachments in the form of a PNG image file that consisted of excerpts of documents. A true and accurate copy of the PNG attachments are attached hereto as **Exhibit B**.

13. I have been informed by Plaintiff that the excerpts contained in the attachments are from the instant litigation.

The Unauthorized Users Performed a Full Data Backup of the Personal Email.

14. On or about September 11, 2017, a full data backup of the Personal Email was performed by someone other than Plaintiff. A true and accurate copy of a screen shot of the created data backup is attached hereto as **Exhibit C**.

McDONALD CARANO
2300 WEST SAHARA AVENUE, SUITE 1200 • LAS VEGAS, NEVADA 89102
PHONE 702.873.4100 • FAX 702.873.9966

15. In performing a full data backup of the Personal Email, the unauthorized users have created and obtained a copy of Plaintiff's entire Personal Email, including all emails sent, received, saved as well as those located in the trash folder.

Recovery Information for the Personal Email was Changed to an Email Address and Phone Number Not Controlled By Plaintiff

16. On or about September 11, 2017 at 2:17 PM, Plaintiff accessed the Personal Email in order to change the recovery email address from "todd@realsocialdynamics.com" to "toddvhan@gmail.com". *See* Exhibit A.

17. Also on or about September 11, 2017, the unauthorized users took the following actions with respect to the Personal Email:

a. At 5:31 PM, the unauthorized users reset the Personal Email recovery email address from "toddvhan@gmail.com" back to "todd@realsocialdynamics.com".

b. At the same time, the unauthorized users removed Plaintiff's recovery phone number ending 3559 from the Personal Email.

c. At 5:36 PM, from a location in Las Vegas, Nevada, using IPv6 address 2600:1011:b05f:d153:513b:9ce:4388:8b9d, the unauthorized users changed the password on the Personal Email.

i. Documents received from Verizon Wireless confirm that the above IPv6 address resolved back to the telephone number 702-600-8317. As indicated below, this is the same telephone number that the unauthorized users added as the recovery phone number. A true and accurate copy of the Verizon Wireless production associating the above IPv6 address with the telephone number 703-600-8317 is attached hereto as **Exhibit D**.

d. At 5:42 PM, from a location in Las Vegas, Nevada, using IP address 174.237.128.12, the unauthorized users added the recovery phone number 702-600-8317 to the Personal Email.

McDONALD CARANO
2300 WEST SAHARA AVENUE, SUITE 1200 • LAS VEGAS, NEVADA 89102
PHONE 702.873.4100 • FAX 702.873.9966

e. At 6:19 PM, from a Mac computer located in Las Vegas, Nevada, using IP address 2600:8801:580:aec0:c531:434:a59d:7b6, the unauthorized users logged into the Personal Email.

f. At 6:43 PM, from a location in Las Vegas, Nevada using IP address 2600:8801:580:aec0:c531:434:a59d:7b6, the unauthorized users removed the recovery phone number 702-600-8317 from the Personal Email.

A true and accurate copy of the Personal Email security log is attached hereto as **Exhibit E**.

18. The subscriber information provided by Verizon Wireless demonstrates that the phone number 702-600-8317 was registered to Defendant Kho from July 19, 2017 to September 29, 2017. A true and accurate copy of the subscriber information provided by Verizon Wireless is attached hereto as **Exhibit F**.

19. This was during the time period that Plaintiff's Personal Email was accessed by unauthorized users.

20. Subsequently, on or about September 29, 2017, the phone number was transferred to defendant Real Social Dynamics, Inc. ("RSD"). *See* Exhibit F.

The Unauthorized Users Forwarded Two (2) Emails to an Email Address Outside the Control of Plaintiff.

21. On or about September 11, 2017, the unauthorized users forwarded two (2) emails from the Personal Email to the email address "toddrsd@hotmail.com" (the "Hotmail Address").

22. Hotmail is an email service provided by Microsoft Corporation.

23. The first email forwarded to the Hotmail Address by unknown third-parties had a subject of "Fwd: Madison video".

24. That email contained an email exchange between Plaintiff and his attorneys, the Nissenbaum Law Group, LLC. A true and accurate copy of the email (redacted to maintain the attorney-client privilege) is attached hereto as **Exhibit G**.

25. The second email forwarded to the Hotmail Address by unknown third-parties had a subject of "Fwd: Owen text 8/14".

McDONALD CARANO
2300 WEST SAHARA AVENUE, SUITE 1200 • LAS VEGAS, NEVADA 89102
PHONE 702.873.4100 • FAX 702.873.9966

McDONALD CARANO
2300 WEST SAHARA AVENUE, SUITE 1200 • LAS VEGAS, NEVADA 89102
PHONE 702.873.4100 • FAX 702.873.9966

26. That email contained screenshots of a text message conversation between Plaintiff and Defendant Cook. A true and accurate copy of the email is attached hereto as **Exhibit H**.

Defendants RSD and Kho are the Unauthorized Users, or the Unauthorized Users are Agents of RSD and Kho Acting at Their Direction.

27. Based on the information obtained from Verizon Wireless, it is clear that the unauthorized users are either Defendants RSD and Kho, or individual agents acting at the direction of RSD and Kho.

28. This conclusion is based upon the fact that the IPv6 address used to change the recovery password of the Personal Email and the recovery phone number entered by the unauthorized users both relate back to a telephone number under the control of Defendants RSD and Kho.

29. Since Defendants RSD and Kho accessed, or directed others to access, the Personal Email without authorization and performed a full data backup of the Personal Email, the contents of Plaintiff's Personal Email are in the possession, custody or control of Defendants RSD and Kho.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

DATED: November 28, 2017.

Ondrej Krehel

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that I am an employee of McDonald Carano LLP, and that on or about the 29th day of November, 2017, a true and correct copy of the foregoing **DECLARATION OF ONDREJ KREHEL, CISSP, CEH, CEI IN SUPPORT OF PLAINTIFF'S *EMERGENCY* MOTION FOR A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION** was electronically filed with the Clerk of the Court by using CM/ECF service which will provide copies to all counsel of record registered to receive CM/ECF notification.

/s/ Jelena Jovanovic
An employee of McDonald Carano LLP

McDONALD CARANO
2300 WEST SAHARA AVENUE, SUITE 1200 • LAS VEGAS, NEVADA 89102
PHONE 702.873.4100 • FAX 702.873.9966

INDEX OF EXHIBITS

Description	Exhibit No.
Artifacts Listing	A
Attachments to Emails in Trash Folder	B
Screen Shot Full Data Backup	C
Verizon Wireless IPv6 Address Information	D
Security Events 9-13-2017	E
Verizon Wireless Number 702-600-8317 Subscriber Information	F
Forwarded Email "Fwd: Madison video"	G
Forwarded Email "Fwd: Owen text 8/14"	H